HEALTH AFFAIRS

TRICARE
Management
Activity

Oversight and Compliance

HIPAA Training: Summer Sessions

TMA Privacy Office

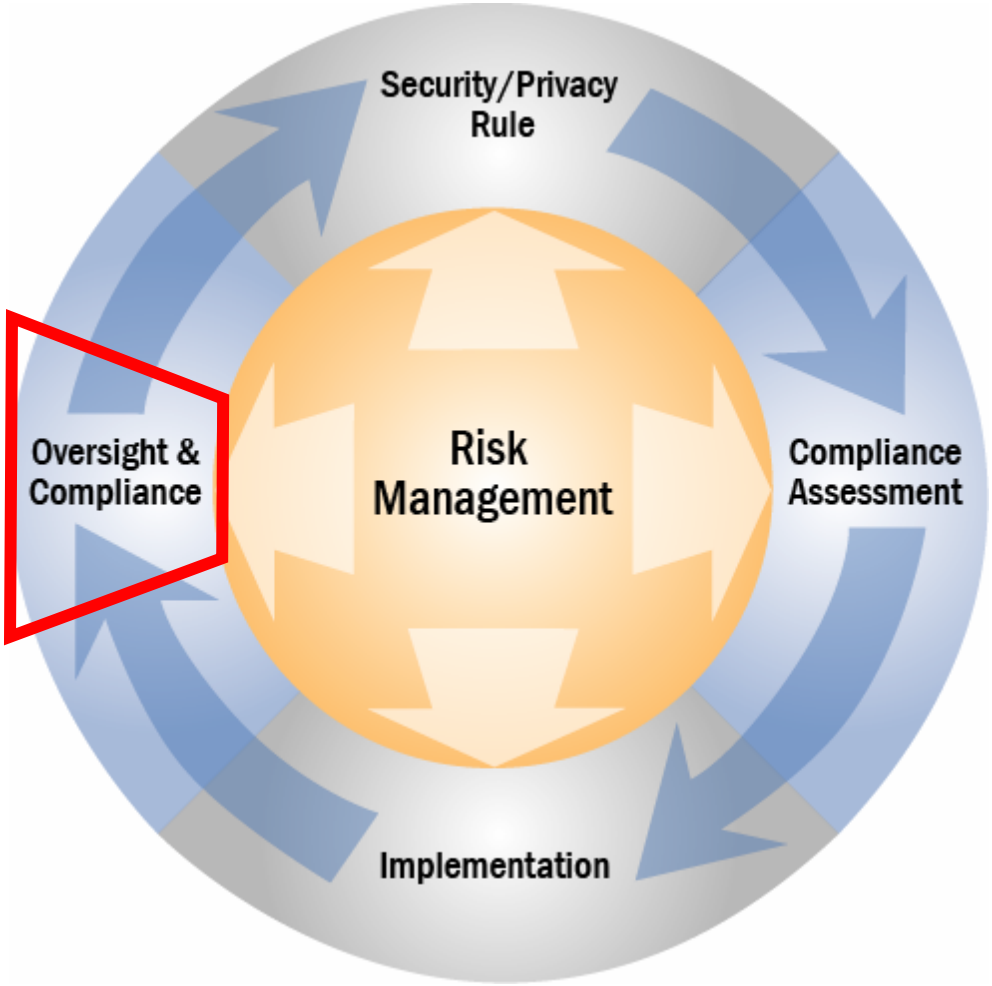
Agenda

- Oversight
- The MHS Organized Healthcare Arrangement
- Compliance Assurance

Training Objectives

- Upon completion of this lesson, you will be able to:
  - Describe the reasons for Oversight
  - Define the MHS Covered Entity
  - List methodologies for Compliance Assurance

HIPAA Implementation Life Cycle



Oversight

"Trust but prove a thing certain"

Objectives

- Upon completion of this module, you will be able to:
  - Describe the requirements and reasons for Oversight
  - List existing oversight responsibilities
  - Explain oversight in the joint organizational structure of the MHS

What is Oversight?

- An independent evaluation of programs and operations to determine whether
  - Management/Internal control systems are adequate
  - Information is reliable, accurate, and available
  - Applicable laws, regulations, and policies are followed
  - Resources are safeguarded and managed economically and efficiently
  - Desired program results are achieved

Multiple Requirements for Oversight (1 of 2)

- Department of Defense
  - Long before HIPAA, DoD had extensive requirements for the use, access and sharing of different classifications of information and the management practices for information systems
  - Difficulties lie in trying to tailor these requirements to medical information in general and PHI in particular
  - Officially audited by both the DoD IG and the individual Service IGs

Multiple Requirements (2 of 2)

- Federal Information Security Management Act (FISMA)
  - Requires organizations to ensure confidentiality, integrity, availability, reliability, non-repudiation, and privacy within the infrastructure and operations of the enterprise
  - Supports compliance with HIPAA Privacy and Security Final Rules by requiring
    - Comprehensive Policies and Procedures for Information Security
    - Training, Education and Awareness
    - Confidentiality, Availability and Integrity of Information
    - Privacy Impact Analyses
    - Technical Controls

Multiple Requirements (cont.)

- Medical Requirements
  - Hospitals
    - Joint Commission on the Accreditation of Healthcare Organizations (JCAHO)
  - Laboratories
    - Clinical Laboratory Improvement Act (CLIA) of 1967
    - College of American Pathologists (CAP)
  - Radiology
    - American College of Radiology (ACR)
- All of these entities review the processes and the practices of the healthcare delivery system

Why Do We Need Oversight? (1 of 3)

- Based on 2003 FISMA reports, DoD received an “D” on the Federal Computer Security Report Card
- FISMA audits conducted by the DoD IG of medical facilities of the MHS showed significant problems with several information security practices (Spring 2003)
- OMB and GAO continue to report no centralized oversight of Federal Agency’s information security programs including DoD

Why Do We Need Oversight? (2 of 3)

- OMB is threatening to reduce IT budgets if security compliance does not improve
- Security requirements continue to tighten and costs for poor security continue to rise

Year	Code Name	Worldwide Economic Impact ($US)
2003	SQL Slammer	$1.0 Billion
2001	Nimda	$653 Million
2001	Code Red(s)	$2.62 Billion
2001	SirCam	$1.15 Billion

Why Do We Need Oversight? (3 of 3)

- Office of Civil Rights (OCR) and the Department of Justice (DOJ) are actively enforcing HIPAA
  - As of July 2004 OCR has received 7,577 HIPAA complaints
  - Closed 57% and referred 108 to DOJ for potential criminal prosecution
  - First-ever criminal conviction for a HIPAA rule violation August 19, 2004
    - Wrongful disclosure of individually identifiable health information for economic gain

Oversight

Tri-Service Organization (1 of 2)

- MHS is a unique organization
  - Component of larger non-medical Federal Agency
  - Has 3 distinct branches of Services and the Coast Guard with individual rules, requirements and ways of doing business
  - All branches are congressionally funded with the medical component receiving separate funding through Health Affairs
- Core mission of the MHS remains the same across all components
  - *to provide medical care to our beneficiaries*!

Oversight

Tri-Service Organization (2 of 2)

- MHS is a joint command….
  - How can the Services ensure that the health data of their patients is adequately protected when patients are able to be seen at multiple facilities in the TRICARE system?
  - How can TRICARE, as the health plan, provide an accounting of disclosures for a patient if facilities maintain separate disclosure accounting systems?
  - How will any one Service be able to provide oversight of IT systems that interconnect across Services?
- …..Oversight is a joint responsibility

Summary

- You should now be able to:
  - Describe the reasons for Oversight
  - List existing oversight responsibilities
  - Explain oversight in the joint organizational structure of the MHS

Organized Healthcare Arrangement

Objectives

- Upon completion of this module, you will be able to:
  - Describe the MHS Covered Entity
  - Define the MHS Organized Healthcare Arrangement
  - Identify the organizations that are part of the Organized Healthcare Arrangement
  - Describe responsibilities for HIPAA Privacy and Security Compliance

Organized Healthcare Arrangement

What is the MHS Covered Entity?

- All DoD health plans and all DoD healthcare providers that are organized under the management authority of, are assigned to or employed by, the TRICARE Management Activity, the Army, the Navy, or the Air Force
- All such covered entities are under the common control of the Assistant Secretary of Defense for Health Affairs (ASD(HA)) and are hereby designated as a single covered entity
- Responsibilities of MHS covered entities shall be construed as responsibilities of the MHS, under the management control of the ASD(HA), and the Director, TRICARE Management Activity

Definition from DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003

Organized Healthcare Arrangement

Members

- DoD has established an “Organized Healthcare Arrangement” that encompasses
  - MHS Covered Entities
  - Elements of the Coast Guard
    - Providers under the control of the Coast Guard and under the Director, Health and Safety Directorate of the Coast Guard
    - The Coast Guard Health Care Program

Organized Healthcare Arrangement

Who is included?

- Consists of the various components of TRICARE
  - Military medical/dental treatment facilities
  - TRICARE purchased care providers
  - Operational medicine (field hospitals, ships, special ops, Marines, etc)
  - TRICARE Management Activity headquarters and the regional offices
  - Service medical headquarters
  - Offices of the Surgeons General

Organized Healthcare Arrangement

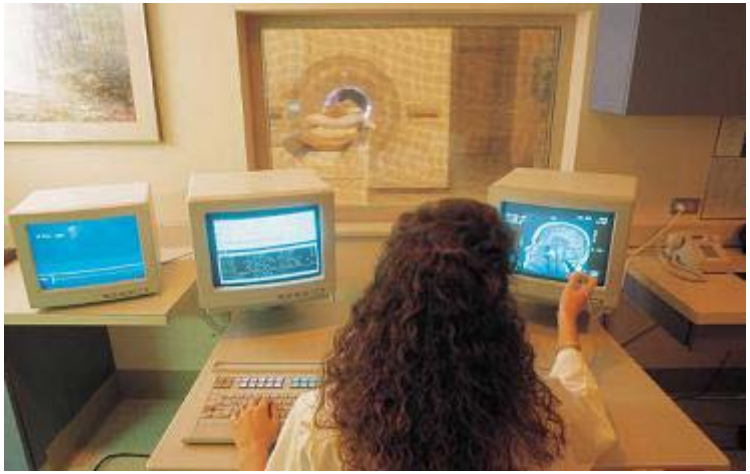
Common Requirements

Common requirements from the HIPAA Privacy and Security Rules

- Internal Audit
- Logical access controls
- Incident procedures
- Security / privacy management
- Sanctioning
- Training
- Assigned responsibility – HIPAA officers
- Physical access controls
- Business Associate Agreements
- Authorization controls
- Personnel Security

Summary

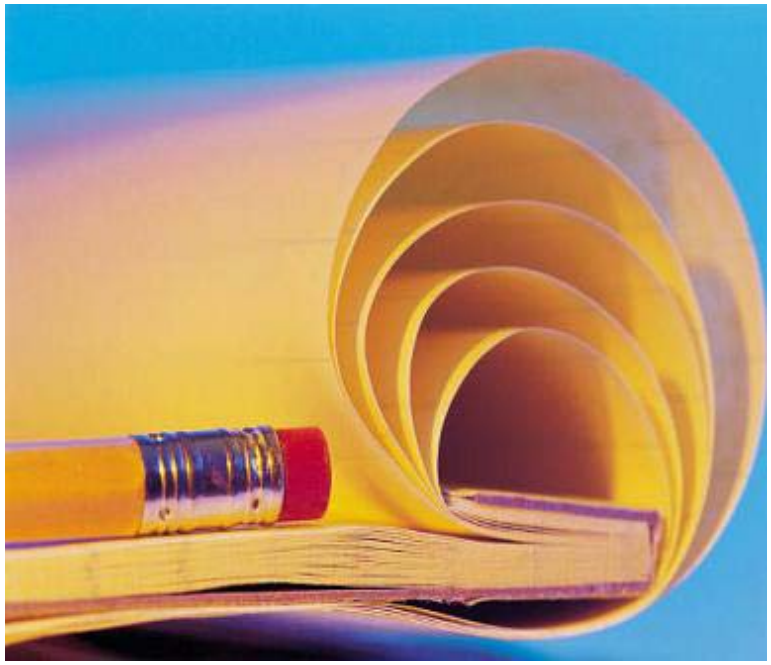
- You should now be able to:
  - Describe the MHS Covered Entity
  - Define the MHS Organized Healthcare Arrangement
  - Identify the organizations that are part of the Organized Healthcare Arrangement
  - Describe responsibilities for HIPAA Privacy and Security Compliance



Compliance Assurance

Objectives

- Upon completion of this module, you will be able to:
  - List methodologies for Compliance Assurance
  - Describe proposed reporting requirements for HIPAA compliance
  - List the tools and resources available for oversight activities



Compliance Assurance Approach (1 of 4)

- Compliance Assurance - **Monitoring and reviewing** performance in areas of compliance risk to ensure
  - Established policies and procedures are being followed
  - Policies and procedures are effective
  - MHS HIPAA data is accurate and reliable

Compliance Assurance Approach (2 of 4)

- Methodologies for Compliance Assurance
  - Initial requirements
    - Reports that provide information on compliance within organizations and across the enterprise
    - Metrics to gauge compliance performance and monitor the progress of HIPAA privacy and security programs

Compliance Assurance Approach (3 of 4)

- Increasing level of detail
  - Program Reviews to ensure that information being reported on HIPAA compliance is accurate and complete
  - POA&M used to identify and monitor privacy and security-related programmatic and system-level weaknesses
  - Metrics to demonstrate the maturity of the organization's HIPAA programs

Compliance Assurance Approach (4 of 4)

NOTE:

- Compliance Assurance requirements for the MHS (including reporting standards) are currently under development by HIPAA Security Integrated Process Team (IPT)
  - Operations Subcommittee is the primary work group for this effort

Proposed Reporting Requirements (1 of 2)

- Frequency
  - Propose quarterly reports for HIPAA security during the implementation phase (July 2004 - April 2005)
  - Propose annual report for HIPAA Privacy
  - After the 2005 compliance date for Security, recommend that both reports be annual or as required by a reported incident or alleged violation

Proposed Reporting Requirements (2 of 2)

- Reports will be at multiple levels of the organization
  - TRICARE Health Plan (MHS)
    - Includes TMA, Army Navy, Air Force, and the Coast Guard
    - Results will be provided to ASD(HA)
  - Service Medical Components/TMA
    - Included entities are at the discretion of the Services and TMA management
    - Results of the reports to be provided to the MHS on a quarterly/annual basis or as requested
  - Military Treatment Facilities
    - Includes clinics and satellite facilities

Military Treatment Facilities

- Recommendations:
  - Training Reports
    - Monthly or as needed to verify compliance
  - Compliance Reports
    - Annual report for HIPAA Privacy Compliance
    - Baseline for HIPAA Security and then quarterly during the implementation phase
    - Annual report for HIPAA Security Compliance after April 2005 deadline
  - Disclosure tracking
    - Perform internal audit on a regular basis to validate procedures
    - Recommendation: Conduct in conjunction with periodic medical record review

Tools for Compliance

- TMA has provided 3 centrally funded and managed tools to facilitate compliance efforts across the MHS
  - Training Tool
    - Plateau's Learning Management System (**LMS**)
    - Quick Compliance Course Content
  - Compliance Tool
    - Strategic Management Systems, Inc **HIPAA BASICS** ™
  - PHI Management Tool (**PHIMT**)
    - HIPAA Accelerator's disclosure tracking tool

Resources

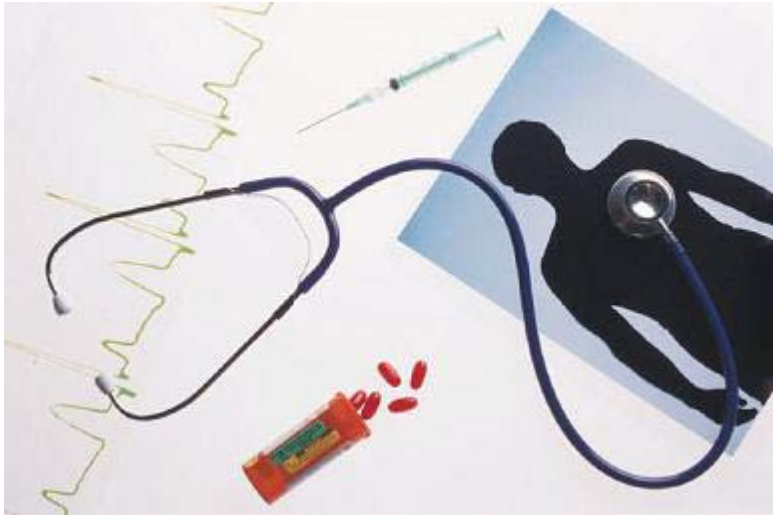
- TMA has provided multiple resources to facilitate compliance
  - Website
  - Information and guidance papers
  - Policies
  - Funding for staff, contracts, and training

Biggest Challenge

- Changing the culture
  - The priority for privacy and security practices for patient information has traditionally been relatively low in most organizations
  - HIPAA rules and the introduction of identity theft and networked data systems are driving the need to change accepted practices

Biggest Challenge

- Need to assess everyday practices such as
  - What information is discussed during Morning Reports?
  - How do your medical records move within and outside of your facility?
  - Determine if practices are truly necessary or are just traditional



Summary

- You should now be able to:
  - List methodologies for Compliance Assurance
  - Describe proposed reporting requirements for HIPAA compliance
  - List the tools and resources available for oversight activities

Summary

- You should now be able to:
  - Describe the reasons for Oversight
  - Define the MHS Covered Entity
  - List methodologies for Compliance Assurance

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- HIPAA Security Rule
- http://www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- HIPAA privacy and security service representatives

HEALTH AFFAIRS

TRICARE
Management
Activity

Please fill out your critique

Thanks!